I/S: A JOURNAL OF LAW AND POLICY FOR THE INFORMATION SOCIETY

National Security Law & Emerging Technologies: Toward a Decisional Framework - Key Takeaways from the ABA-OSU Symposium and Jirga

JAMES E. BAKER*

CONTENTS

* Chair, ABA, Standing Committee on Law and National Security (2015-2018); Professor Syracuse University College of Law and Maxwell School of Citizenship and Public Affairs and Director of the Institute of National Security and Counterterrorism. This article was written while serving as the Robert Wilhelm Fellow, at the Center for International Studies, Massachusetts Institute of Technology. Baker is a retired Judge and Chief Judge of the United States Court of Appeals for the Armed Forces and a former Legal Adviser to the National Security Council.

I. INTRODUCTION

This essay is intended to perform two tasks. First, it describes the imperative behind the annual "National Security, Emerging Technologies, and the Law" Symposium jointly sponsored by the American Bar Association ("ABA") and The Ohio State University Moritz College of Law ("OSU"). Toward this end the essay introduces the reader to artificial intelligence, quantum computing, and synthetic biology along with their national security applications and implications. Second, the essay identifies eight Symposium takeaways, key points that should inform the application of national security law and process to emerging technologies going forward. The intent of this article (as was the intent of the Symposium) is to establish a framework for discussion and decision, with the hope that the next conference will build upon these conclusions, not repeat them.

II. EMERGING TECHNOLOGIES AND NATIONAL SECURITY

Emerging technologies, like artificial intelligence (AI), quantum computing (QC), and synthetic biology, offer great commercial and humanitarian promise. Artificial intelligence applications, for example, are a valuable tool in treating cancer, with better than human accuracy in identifying tumors. Alone, or paired with the computational capacity of quantum computing, AI promises to help cure diseases as well as to stem environmental degradation, in addition to empowering driverless cars, delivering packages, and running kitchen appliances. Likewise, synthetic biologics, such as tools used to alter gene sequences, can be used to drive genetic selection toward more fertile crops or to sterilize and eliminate disease vectors, rather than defer those goals to the less certain and time-consuming process of natural selection.

These same technologies, however, will also impact, and likely transform, national security in both positive and negative ways. Stephen Hawking said, "The rise of powerful AI will be either the best

or the worst thing to ever happen to humanity."[1] A 2017 study concluded that "Future progress in AI has the potential to be a transformative national security technology, on a par with nuclear weapons, aircraft, computers, and biotech."[2] In 2017, China's State Council approved a plan to make China the world leader in the AI field by 2030, targeting a gross output of $150 billion for the core AI industry.[3] Vladimir Putin has declared "the one who becomes the leader in this sphere will be the ruler of the world."[4] No wonder AI is at the center of the Department of Defense's Third Offset Strategy, using technology to offset the geographic, asymmetric, and numerical advantages of potential adversaries.[5]

In short, AI is recognized as a national security tool by critical actors. It is here and here to stay. Quantum computing, in turn, has the potential to exponentially speed up this process. It also has the potential to transform the world of encryption, potentially unlocking virtually all current encryption applications, applications that protect nuclear codes, financial transactions, and every-day communications; unless of course, quantum computing leads to unbreakable codes first.

---

[1] Stephen Hawking, Professor, Speech at the Launch of the Leverhulm Centre for the Future of Intelligence, Cambridge, England. (Oct. 19, 2016), https://www.cam.ac.uk/research/news/the-best-or-worst-thing-to-happen-to-humanity-stephen-hawking-launches-centre-for-the-future-of [https://perma.cc/96G4-CSB3].

[2] GREG ALLEN & TANIEL CHAN, ARTIFICIAL INTELLIGENCE AND NATIONAL SECURITY, BELFER CENTER FOR SCIENCE AND INTERNATIONAL AFFAIRS STUDY 1 (Jul. 2017), https://www.belfercenter.org/sites/default/files/files/publication/AI%20NatSec%20-%20final.pdf [https://perma.cc/LH8D-U67W].

[3] JEFFREY DING, DECIPHERING CHINA'S AI DREAM: THE CONTEXT, COMPONENTS CAPABILITIES, AND CONSEQUENCES OF CHINA'S STRATEGY TO LEAD THE WORLD IN AI, UNIVERSITY OF OXFORD FUTURE OF HUMANITY INSTITUTE 7 (Mar. 2018), https://www.fhi.ox.ac.uk/wp-content/uploads/Deciphering_Chinas_AI-Dream-1.pdf [https://perma.cc/789C-THMW].

[4] *Putin: Leader in Artificial Intelligence Will Rule World*, CNBC (Sep. 4, 2017),

https://www.cnbc.com/2017/09/04/putin-leader-in-artificial-intelligence-will-rule-world.html [https://perma.cc/TX97-HVNB].

[5] *See, e.g.*, Bob Work, Deputy Sec'y of Def., Speech at the Dep't of Def. CNAS Def. Forum, (Dec. 14, 2015), https://www.defense.gov/News/Speeches/Speech-View/Article/634214/cnas-defense-forum/ [https://perma.cc/5S8S-67KN]; *see also*, U.S. DEP'T OF DEFENSE, SUMMARY OF THE 2018 NATIONAL DEFENSE STRATEGY OF THE UNITED STATES OF AMERICA: SHARPENING THE AMERICAN MILITARY'S COMPETITIVE ADVANTAGE 3 (2018), https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf [https://perma.cc/P8B4-SLUB].

There is an "arms race" here as elsewhere, not just between nations, but between those who research for offensive purposes and those who do so for defense.

The confluence of Big Data, algorithm design, computational capacity, and the Internet of Things has spurred financial incentives to research and develop AI applications. It has also increased societal and security vulnerabilities, or as some say, "attack surfaces." There is some debate about how and whether these technologies will meet their potential, but mostly the debate is about when this will occur. This makes the study of emerging technologies and national security law imperative, and imperative now. Informed law is most likely to guide decision-makers to preferred outcomes before decisions are made and budgets spent, rather than the current default options of "waiting to see" or "hoping for the best." Nations are also more likely to agree to legal and ethical limitations before real or perceived security advantages are gained.

III. THE THREE PURPOSES OF NATIONAL SECURITY LAW

National security law serves three purposes, or rather it can serve three purposes if crafted well and wielded wisely. It provides the substantive authority to act, as well as the left and right boundaries of that action. Law, including executive direction, provides essential process. There is nothing inherently good or bad about process. Good process is timely, contextual, and meaningful and results in better national security outcomes. That is because good process, among other things, better fuses intelligence, identifies options, mitigates risks, provides for unity of command and message, and addresses the pathologies of national security decision-making, like secrecy and speed.

Finally, law provides national security as well as legal values. For example, the humane treatment of prisoners in war is both a legal value (Geneva Common Article 3) and a national security value (humanely treated prisoners are more likely to provide information). Often, debates about the authority of the law, such as those over Section 215 of the PATRIOT Act and Section 702 of the FISA Amendments Act of 2008, are proxy debates about which values in law and national security we should emphasize or privilege. In the field of emerging technologies, many of these values are expressed in Constitutional terms, including the structural framework of the Constitution (federalism and separation of powers) and within the First, Fourth, and Fifth Amendments.

All three purposes of law are in flux and in play with emerging technologies. We tend to teach what we know and are comfortable with. And, in government, we tend to focus on the immediate and the crisis, rather than tomorrow's needs, which might avert future crisis. Even though there has been a lot of discussion and debate about cyberspace and the role of private actors and privacy on the Internet, we have, nevertheless, focused on the tactical questions at the expense of the strategic. We do not need another conference about Section 702.

The bottom line is the United States has not effectively addressed and resolved questions of authority, process, or values regarding emerging technologies. It is now time to focus on the big technologies that will transform national security in the century ahead.

What are those technologies? How will they impact national security? Further, how should we regulate their use, mitigate their risks, and utilize their promise, and what are the limitations?

IV. THE BIG THREE

There are many technologies that will impact national security and foreign relations in the century ahead. Some such technologies do not yet exist. Three do, and we know now that they will be transformative: Artificial Intelligence, Quantum Computing, and Synthetic Biology.

A. *Artificial Intelligence*

AI is hard to define because it reaches multiple fields and subfields of research and development, including algorithms, big data, and machine learning. The Stanford 100 Year Study defines AI as "a science, and a set of computational technologies, that are inspired, but typically operate quite differently from, the way people use their nervous systems and bodies to sense, learn, reason, and take action."[6] This definition encompasses AI's myriad parts and directions. At present, AI has come closest to its promise and demonstrated the most human like machine intelligence (HLMI), or better, regarding data aggregation and pattern recognition.

---

[6] PETER STONE, ET AL., ARTIFICIAL INTELLIGENCE AND LIFE IN 2030 4 (2016), https://ai100.stanford.edu/sites/default/files/ai100report10032016fnl_singles.pdf [https://perma.cc/2PU5-VT35].

AI has many national security applications, or potential applications. In the military area, these include: Offensive and defensive swarm technology, autonomous and semi-autonomous weapons, training, and logistics. Moreover, any military task that involves danger, repetition, or is undermined by human fear and fatigue might, but not necessarily, be better performed by AI enabled technology.

In the intelligence area, AI has obvious capacity to aggregate, sort, and weigh data, making it ideal for pattern recognition, anomaly detection, and link analysis. For these same reasons it could prove, and is proving, a useful tool for authoritarian regimes seeking to accomplish the same goals for social control reasons or to undertake foreign influence operations. In the decisional area, AI is, or will be, a useful tool for fusing information, predicting outcomes, and modeling policy choices.

AI has been around in concept since Alan Turing, Bletchley Park, and the Imitation Game. The first academic AI conference occurred in 1956.[7] What has transformed the field in recent years is the advent of computational capacity, Big Data, algorithms, neural networks, and machine learning. AI's commercial applications and promise guarantees steady R & D funding going forward. However, AI's promise also comes with substantial security risks. These risks include the loss of control that comes with autonomous and semi-autonomous systems, the challenge of human interfaces with complex technology, and the potential for unintended results. AI could also result in decisional pathologies generated by the absolute speed AI offers to cyber operations and, more generally, decision-makers confronting the faster fusion of intelligence and new models of weighted predictable policymaking. Furthermore, AI can contribute to instability, conflict, economic displacement, and the sorts of pathologies generated by an arms race mentality discussed below.

B. Quantum Computing

The "what" and the "why" of quantum computing is easier to explain than the "how" and the "when." Classical computers, or current computers as we know them, use electricity, transistors, and

---

[7] Rockwell Anyoha, *the History of Artificial Intelligence*, HARV. UNIV., THE GRADUATE SCH. OF ARTS AND SCI.: BLOG, SPECIAL EDITION ON ARTIFICIAL INTELLIGENCE (Aug. 20, 2017), http://sitn.hms.harvard.edu/flash/2017/history-artificial-intelligence/ [https://perma.cc/4QRH-FTQ8].

circuits to translate information into binary bits conveying information and commands represented as zeros and ones. Over the years, engineers have made smaller and smaller silicon chips with more and more transistors allowing ever greater data to be stored and processed in computers. That is what allows the computer chip in the iPhone 5 to store 2.7 times the computational capacity as a 1985 Cray-2 Supercomputer.[8] But the size and storage capacity of electricity driven computer chips is finite and approaches quickly. Enter quantum computing.

Quantum computing (QC) seeks to use light rather than electricity and the principles of quantum physics to process data (quantum physics addresses subatomic particles). The basic building block of QC is the qubit, or quantum bit. Subatomic particles have the capacity to exist in more than one state—in wave or particle form. That means that instead of the essential computational building block one-bit that can represent a one or a zero, two qubits could represent four possible values at once: OO, O1, 10, and 11. Because qubits exist in more than one state, they can both handle more data than a classical binary bit, and they can parallel compute in their multiple states. The more qubits that are used, the greater and faster the computational power, so much so that quantum computers could potentially be more powerful than classical computers by a magnitude of billions.[9] So far, so good.

That leads to the "why." With that much computational capacity, it means you can accomplish tasks using brute force computation that would take classical supercomputers years to accomplish, like breaking codes, or are simply not possible to do, like solving the molecular riddle of certain diseases. Quantum computing will also

---

[8] *Processing Power Compared: Visualizing a 1 trillion-fold increase in computing performance.*, EXPERTS EXCHANGE, (Last Visited Nov. 18, 2018), https://pages.experts-exchange.com/processing-power-compared [https://perma.cc/YH5J-LSGL].

[9] *See*, Cade Metz, *IBM Is Now Letting Anyone Play With its Quantum Computer*, WIRED (May 4, 2016), https://www.wired.com/2016/05/ibm-letting-anyone-play-quantum-computer/ [https://perma.cc/D9EZ-DUJE]; Michael Nielsen, *Quantum Computing for Everyone*, MICHAEL NIELSEN (Aug. 28, 2008), http://michaelnielsen.org/blog/quantum-computing-for-everyone/ [https://perma.cc/93E6-CTLB]; Tom Abate, *Stanford Team Brings Quantum Computing Closer to the Reality With New Materials*, STANFORD NEWS (May 9, 2017), https://news.stanford.edu/press-releases/2017/05/09/new-materials-brg-closer-reality/ [https://perma.cc/2477-VC8V]; Michael J. Biercuk & Richard Fontaine, *The Leap into Quantum Technology: A Primer for National Security Professionals*, WAR ON THE ROCKS (Nov. 17, 2017), https://warontherocks.com/2017/11/leap-quantum-technology-primer-national-security-professionals/ [https://perma.cc/8823-KPPK].

ignite and accelerate AI. The security advantages to a first mover are enormous, especially if one's adversaries are not yet aware you have broken their encryption, one has stored past communications to decipher, or it is too costly to securely retrofit infrastructures even when the QC security risk is known. Imagine the risks if QC ends up in the wrong hands, such as the threat to air travel, infrastructures that rely on encryption to protect operating systems (energy, water), or data and communications, like the financial industry.

The "how" is more complicated for non-specialists to understand. I am not sure scientists and engineers fully understand it either; otherwise, we would likely already have quantum computers. Quantum computing relies on two concepts: supposition and entanglement. Supposition is the capacity of subatomic particles to exist in two states seemingly at once. Entanglement is a concept in quantum physics that posits that two particles exist in a state of interaction such that they can only be understood and measured in relation to each other. Among other things, this allows the parallel processing of data and thus faster processing. However, one needs to understand quantum physics to fully appreciate how exactly quantum computing works or might work. I do not and will not pretend otherwise here. But I do appreciate in concept why it is difficult to isolate and measure particles and light waves in subatomic form, based on their size, speed, and changing state. They are unstable. Therefore, to use a qubit for computational purposes one needs to isolate and measure the qubit in a predictable state of supposition and entanglement. This is where much of the research is being conducted. One way to slow down and isolate particles for measurement is apparently with extremely cold temperatures, like absolute zero, the lowest temperature that is theoretically possible. Another way is to try and find different and more precise ways to measure qubits with lasers.

That brings us to "when." IBM has produced a 20-qubit quantum computer, which is available for cloud computing and public research. IBM has also produced a 50 Qubit computer, which in theory, comes much closer to realizing the potential of quantum computing. However, the quantum state was "preserved for 90 microseconds—a record for the industry, but still an extremely short period of time."[10]

---

[10] Will Knight, *IBM Raises the Bar with a 50-Qubit Quantum Computer*, MIT TECH. REV. (November 10, 2017), https://www.technologyreview.com/s/609451/ibm-raises-the-bar-with-a-50-qubit-quantum-computer/ [https://perma.cc/2L3F-FDRW].

Less certain is the timing of and feasibility of a stable qubit computer being scaled up to the number of qubits to unlock the potential promise of quantum computing. The, or a, challenge is handling the size of the mathematical equations and variables that are generated by qubit driven computers. "More than a million numbers are needed to describe a 20-qubit quantum computer. The contrast with conventional computers is striking – a conventional 20-bit computer needs only 20 numbers to describe it."[11] It may be that it takes quantum computing to solve quantum computing.

Given the potential national security advantages and risks presented by QC and the amount of academic, industry, and governmental money being invested into its research and development, I would not bet against its arrival in my national security lifetime. We better be ready.

C. Synthetic Biologics

Synthetic biology is the field of science addressed to the creation of synthetic (or artificial) biological pathways, organisms, and devices as well as the manipulation of natural occurring pathways, organisms, and devices.[12] A biological pathway is a series of molecular interactions that lead to a result. For example, an enzyme used in the production of synthetic rubber, which otherwise is produced only in rubber trees, a limited natural resource.[13] Synthetic biology has been used to make vaccines and biosensors. CRISPR is the best-known example of a biological tool used to manipulate naturally occurring biology through genetic manipulation by isolating, cutting, and reordering DNA molecules.

---

[11] Nielsen, *supra* note 9.

[12] *See*, Wikipedia, *Synthetic Biology*, for an introduction to the disciplines and technologies involved in synthetic biology, then, move on to MIT's Kenneth Oye, among other scholars. *See*, *e.g.*, KENNETH OYE, ET AL., ON REVISION OF THE COORDINATED FRAMEWORK FOR THE REGULATION OF BIOTECHNOLOGY, MASSACHUSETTS INSTITUTE OF TECHNOLOGY (Mar. 22, 2016) https://poet.mit.edu/sites/default/files/images/ON%20REVSIONOFCF2016-03-22-FINAL.pdf [https://perma.cc/25RY-JA5U]; *see also*, Kenneth Oye, et al., *Regulating Gene Drives*, 345 SCIENCE 626, 626-28 (Aug. 8, 2014).

[13] BIOTECHNOLOGY INNOVATION ORGANIZATION, *Current Uses of Synthetic Biology*, (May 31, 2018), https://www.bio.org/articles/current-uses-synthetic-biology [https://perma.cc/CN2H-LXUW].

There are many positive examples of how synthetic biology can potentially contribute to the common good, such as through the creation of biologics that can identify and attack cancerous cells before they are detectable using existing diagnostic methods. In the national security sphere, synthetic biology could be harnessed to attack diseases or prevent the spread of diseases that create conditions of instability, conflict, and economic barriers. It is obvious as well that synthetic biology can be used to make new chemical weapons and biological warfare agents for which no known antidotes or prophylactics currently exist. Despite the general prohibition of biological and chemical weapons, states (e.g., Russia, Syria, North Korea) and non-state actors (e.g., Aum Shinrikyo 1995) may still seek to use synthetic biology as a weapon. Gene drives in turn can be used for good — for instance, to eradicate a disease carrying insect — or for bad — such as, to destroy crops, or to introduce pathogens that will only affect certain genetic characteristics associated with a particular race or ethnicity. Lawyers and ethicists also debate the limits that should apply to the creation of new life forms and the questions regarding access and availability to disease cures and treatments.

Certainly, there are other emerging technologies of national security importance. One example is blockchain, a perpetual train of encrypted virtual currency transactions, which can serve as a virtual wallet or receipt. Additionally, depending on the definition of AI, there are numerous subfields warranting national security study, like autonomous weapons systems. Lawyers have a professional duty to competently and diligently represent their clients, and they cannot do this very well without understanding the technology that informs their work and safeguards their confidences. For the ABA-OSU Symposium, we focused on the two leading digital technological fields, AI and QC, because of their potential to transform national security and because of OSU's and *I/S*'s focus on digital issues.

V. WHY AN ABA-OSU SYMPOSIUM AND JIRGA ON AI AND QC?

One of the missions of the ABA Standing Committee on Law and National Security is to educate the public and the profession on the interplay between law and national security. In 2010, the Committee started holding a Lawyers Jirga for teachers and professionals to facilitate and explore methodologies for teaching national security law as well as to bridge the gap between civilian and military teaching methods. The name derives from the term for a Pashtun meeting of Elders where decisions on governance and law are often addressed

and settled in Afghan society. The Ohio State University (OSU) Symposium was the ABA's eighth Jirga and the first addressed specifically to technology.

In concept, the Jirga has three objectives. First, the Jirga aims to apply innovative and best practice methods to teaching the national security law and policy. Second, it serves as a bridge to the larger community of national security actors, reaching practitioners and thought leaders outside the Washington Beltway. The Jirga on homeland security, for example, took place in Oklahoma City at the site of, and on the twentieth anniversary of, the 1995 Alfred P. Murrah Federal Building bombing. After all, the topic is national security and our Committee derives from the American Bar Association. Third, the Jirga is intended, as is the work of the Committee itself, to identify and focus the national security legal community on over-the-horizon issues and to prepare today's lawyers to meet tomorrow's challenges.

All three of these factors made the Moritz College of Law at the Ohio State University an excellent partner for a Symposium and Jirga on Emerging Technologies and National Security Law. To start, OSU is one of the Nation's leading research universities. Most of the research and development in emerging technologies is occurring at research universities, like OSU, Federally Funded Research Centers, and in industry (at times, it seems, the government is more spectator than participant). The law school also has a reputation for the study of digital technology. The fact that the Symposium was supported by a leading journal, *I/S: A Journal of Law and Policy for the Information Society*, ensured that the voices heard at the Conference would later amplify and reach a larger audience. OSU is also increasingly known for its emphasis on experiential teaching through its national security simulation. Finally, the University has a longstanding tradition of honoring and contributing to public service, reflected in, among other places, its military history department and Corps of Cadets.

Having explained why the Committee has focused on emerging technologies and done so at OSU, the remainder of this article turns to the core takeaways and themes from the Symposium. In identifying the key takeaways, my hope is that the next conference will build upon these conversations and conclusions, not repeat them. One key takeaway is that any successful effort to understand and regulate the applications and implications of new technologies will have to bridge six constituencies and do so vertically and horizontally. Those constituencies are: technology, policy, law, industry, academia, and government.

VI. KEY TAKEAWAYS

A. National Security Practitioners must understand all three legs of the Emerging Technology Stool — Technology, Policy, and Law

It is now trite to say, but nonetheless true, that national security in the digital age rests upon a three-legged stool of policy, law, and technology. National security practitioners tend to be proficient in two of these three areas. To most effectively practice law or policy in this space, however, one needs to be proficient in all three disciplines, including the technical aspects of emerging technologies. Why does this matter?

First, without understanding the technology, policymakers and lawyers may opt for policy and legal frameworks with unintended consequences or that are quickly outdated. Second, they may miss opportunities to apply technical solutions to problems that might otherwise seem like intractable policy or legal problems, like those associated with attribution or accountability. Third, it is hard to understand and thus address the due process concerns associated with AI, like neural networks operating in the "black box" of deep machine learning, without understanding the process by which neural networks sort, weigh, and predict outcomes. Fourth, technical comfort is important to credibly bridging the camps and constituencies integral to effectively craft law and policy directed to industry and academia, and not just government actors.

Applying law to policy is very hard if you do not understand the parameters of the policy to which you are applying law. The same is true of technology. This means that law schools and policy schools need to move beyond their comfort zones and teach more about technology, which necessarily means less about something else. This may require new hires across generations, the use of additional adjuncts, or tapping into the advantages of interdisciplinary universities.

B. Communicate in Plain English

Lawyers apply law to facts and explain complex areas of the law to policymakers while doing so. The best lawyers do so in plain English so that policymakers not only understand what the law is, but why the law is the way it is, and how the law might apply in different responses to evolving and changing facts. The best lawyers tell policymakers what it is they need to know, not what it is the lawyer knows.

Technologists need to learn to do the same if they do not already know how to do so. The policy answer to a policy question about algorithms is not a mathematical equation. And if the answer takes a white board to explain, it will likely not translate well into legislative language or policy-talking points. As with lawyers, the trait that is most impressive to a security specialist is not how much you know or how smart you are, but how smart you are in conveying to policymakers what it is they need to know.

If you want to test this proposition, the lawyer should ask of the technologist, "If I were in court and you were my expert, how well would you explain the scientific basis for the technology upon which the evidence you are about to offer is based?" As some lawyers will recognize, this question is rooted in *Daubert* and *Kuohmo Tire,* the Supreme Court cases providing the framework for authenticating and validating new scientific methods before admitting evidence in court based on these methods. The policymaker might ask, (1) "If I were explaining this technology to the Secretary of State or the President, would I want this technologist to do so?"; (2) "How would or should he or she spend their five minutes?"; or (3) "Would he or she grasp and present the policy implications? Or, just the mechanics of how it all works?"

If you want to take this thought for a dry run, ask your technologist to explain Quantum Computing in four sentences or less and do so without reference to equations or formulas.

C. Technology Involves Human Choice, It Does Not Remove It

There is a tendency to treat emerging technologies as inexorable and inevitable in their reach, seemingly immune from human control or influence. This may not be a surprise in a field that includes robots, autonomous weapons, debates about whether there should be a human-in-the-loop, and where and how, if so. However, the human factor was emphasized repeatedly during the Symposium as speakers noted in paraphrased form here and further below:

It is a matter of human choice to opt in or out of default privacy settings.[14]

AlphaGo did not defeat Lee Sokol in a game of Go, a team of software engineers did.[15]

It is humans who will resolve competing values many technologies present, or who will decide to default to choices made by software engineers.[16]

Compliance with law is a human task.[17]

Make no mistake about it, emerging technologies present human choices, or as one discussant put it, "Machines do not decide things of their own free will."[18] Lawyers, technologists, and policymakers need not stand by and watch; they control the outcome and they are responsible for the outcome. Technology is not a runaway train; it is a train with human conductors who can either step up and conduct or sit back and hope the train does not jump the rails. The governance question is this: who should or will decide to conduct, and in what manner?

---

[14] Peter Weinberger, Software Engineer, Google, The New School, Panelist at the 2018 I/S: A Journal of Law and Policy for the Information Society Symposium: National Security, Emerging Technologies, and the Law, Panel: The Future of Digital Intelligence: Artificial Intelligence, Cyber, Quantum Computing, and Cryptography Part II at 42:56 (Mar. 23, 2018).

[15] Peter Asaro, Assoc. Professor, School of Media Studies, The New School, Panelist at the 2018 I/S: A Journal of Law and Policy for the Information Society Symposium: National Security, Emerging Technologies, and the Law, Panel: Artificial Intelligence and National Security at 1:15:57 (Mar. 23, 2018).

[16] Judge James E. Baker, Jeff Alstott, Program Manager, Intelligence Advanced Research Projects Activity (IARPA), 2018 I/S: A Journal of Law and Policy for the Information Society Symposium: National Security, Emerging Technologies, and the Law, Panel: Emerging Technologies, National Security, Law and Ethics: A Conversation (Mar. 24, 2018).

[17] Allan Schuller, Assoc. Dir., Stockton Ctr. For the Study of Int'l Law, Panelist at 2018 I/S: A Journal of Law and Policy for the Information Society Symposium: National Security, Emerging Technologies, and the Law, Panel: Artificial Intelligence and National Security (Mar. 23, 2018).

[18] *Id.*

1. *Corporate Identity and Responsibility*

A number of speakers observed that we have lost a sense of citizenship at the individual and the corporate level."[19, 20] One speaker stated that he found no American flags flying or evident at Facebook.[21] Another speaker stated that boardrooms have become their own countries.[22] Whether or not these observations are purely anecdotal in the same manner that the evident patriotism of corporate participants at the Symposium is anecdotal, they do reflect ambivalence about corporate identity and responsibility. Emerging technologies will place additional pressure on corporations to define their identity and responsibility when values like privacy, national security, free trade, and shareholder value compete. As evidenced by efforts to monetize data and questions over how Russia utilized (and utilizes) Facebook and other social media platforms for influence operations, there are no agreed norms of responsibility, let alone laws, for U.S. corporations. Questions abound:

What responsibility do U.S. corporations have to protect national security?

How should one define "U.S. Corporation"?

Should the responsibility be defined in a passive or an active way?

---

[19] Diana S. Dolliver, Assistant Professor and Academic Dir., Joint Electronic Crimes Task Force, Univ. of Ala. Dep't of Criminology and Criminal Justice, Herb Lin, Senior Res. Scholar for Cyber Pol'y and Sec., Ctr. for Int'l Sec. and Cooperation and Hank J. Holland Fellow in Cyber Pol'y and Sec., Hoover Inst., Stan. Univ., Robert S. Litt, Former Gen. Couns. to the Off. of the Dir. of Nat'l Intelligence and Of Couns., Morrison & Foerster, 2018 I/S: A Journal of Law and Policy for the Information Society Symposium: National Security, Emerging Technologies, and the Law, Panel: Issues of Government Organization, Capacity and Accountability (Mar. 23, 2018).

[20] Harvey Rishikof, Former Chair, Dep't of Nat'l Sec. Strategy and Professor of L. and Nat'l Sec. Stud., Nat'l War Coll., Panelist at 2018 I/S: A Journal of Law and Policy for the Information Society Symposium: National Security, Emerging Technologies, and the Law, Panel: The Future of Digital Intelligence: Artificial Intelligence, Cyber, Quantum Computing, and Cryptography Part II at 1:03:00 (Mar. 23, 2018).

[21] *Id.* at 1:03:32.

[22] *Id.* at 1:03:20.

Should responsibility be defined in law? Determined on a case-by-case basis?

Should corporations be required to adopt minimum solutions or optimum solutions to address security needs and threats?

How, if at all, should answers be different for different technologies? Or, with respect to conduct occurring in the cyber domain?

Who pays, or as one participant stated, "who takes the monetary hit"[23] for doing the right thing?

Questions of corporate responsibility are particularly pronounced in the supply chain context.

2. *Address Supply Chain Risk Management*

Multiple speakers across industry, academia, and government alluded to supply chain risk management (SCRM). Indeed, SCRM brings many of the themes of the Symposium together, such as those of corporate identity and purpose, and arms race risks and security.

Supply chain risk is defined by the Office of the Director of National Intelligence with reference to the Intelligence Community as "the management of risk to the integrity, trustworthiness, and authenticity of products and services within the supply chain. It addresses the activities of foreign intelligence entities and any other adversarial attempts aimed at compromising the IC supply chain, which may include the introduction of counterfeit or malicious items into the IC supply chain."[24] Of course, the definition applies generally to industry as well. Supply chain risk occurs constantly and consistently across the life cycle of a technology's use from manufacture, to production, to assembly, to refurbishment. It is found

---

[23] Herb Lin, Senior Research Scholar for Cyber Pol'y and Sec., Ctr. for Int'l Sec. and Cooperation and Hank J. Holland Fellow in Cyber Pol'y and Sec., Hoover Inst., Stan. Univ., Panelist at 2018 I/S: A Journal of Law and Policy for the Information Society Symposium: National Security, Emerging Technologies, and the Law, Panel: Issues of Government Organization, Capacity and Accountability 56:50 (Mar. 23, 2018).

[24] Office of the Dir. of Nat'l Intelligence, Intelligence Cmty. Directive No. 731, Supply Chain Risk Mgmt. (2013), https://www.dni.gov/files/documents/ICD/ICD%20731%20-%20Supply%20Chain%20Risk%20Management.pdf [https://perma.cc/JEF9-GKX8].

in software, hardware, and the "humanware" that operates and maintains equipment.

The Symposium identified any number of ways to address risk management. These include: The adoption of back-up plans and resilient systems; designing systems based on the principle of suspicion, that is, assuming the risk of penetration; risk scoring; protection plans; industry or component standards; provenance and authenticity standards; and testing. The Symposium also addressed ways to incentivize the adoption of these risk management tools. These include: litigation, consumer pressure, taxation incentives, and insurance policy and pricing.

Beyond any specific suggestions, the core message here was to do something. Pick something to protect, protect it, and learn from the experience about the intended and unintended consequences of doing so. That leads to the next general theme.

3. *Do Something*

Too often it seems tough problems sit and linger. They are too hard. There are too many constituencies. There are too many interests. There are no obvious or good solutions. For sure, competing values are sometimes best sorted out in context, rather than with generalized solutions embedded in law, such as those tradeoffs that might occur between open trade and national security.

But consider how long the United States Government has debated cyber questions like:

Which agency or agencies should take the lead in response to cyber security? Or,

When does a cyber-attack amount to an armed attack for the purposes of policy response, international law, and the law of armed conflict? Or,

What should the government tell industry about the threat of attack in advance?

These questions were identified at the advent of the digital age in the 1980s and 1990s. They are still debated today with only marginal development in the past two decades. Sometimes it is better to do something, to take a position, evaluate the results, and then adjust,

than to default to voluntary "best practices" or the lifeboat mentality of "every man for themselves."

The complexity of regulating emerging technologies and the number of disparate stakeholders can make this space feel ungovernable. If the United States government does not take a position, or act to fill the vacuum on what law does or should apply to emerging technologies, the answers will arrive by default. Legal policy will be determined in a decentralized manner by individual actors, considering the specific interests of those actors. Google will make policy decisions with national security impact based on corporate responsibilities and goals. Likewise, disputes will be resolved not through the legislative process or rulemaking process - where a full range of policy views and outcomes may be addressed - but through litigation where the interests of individual parties are paramount, and the adversarial process drives parties to zero-sum rather than optimal goals and outcomes.

4. *Parkinson's Law meets Moore's Law*

When it comes to emerging technologies, it seems like there is a lot of law. It is just not the sort of law that is taught in law schools or that a lawyer might recognize as law. Those who will, can, or shall, craft our legal and ethical response to emerging technologies should do so conscious of this "law." There is:

Parkinson's Law: Parkinson's Law is the name of the book by a professor at the University of Malaya about bureaucratic process. In 1957, Northcote Parkinson first observed that work fills the space allocated to perform it, among other abiding bureaucratic observations. Parkinson's "law" applies to emerging technologies, because there is no time at which point it is certain that emerging technologies will come to transform national security. Therefore, the task of providing a governing framework will linger. Policymakers will push the point of decision and choice further out, until a crisis or Sputnik moment forces action. But law is harder to craft in crisis and values harder to hold. We should debate and install a legal framework now.

Moore's Law: Moore's Law is named for Intel co-founder Gordon Moore who in 1965 predicted that the number of transistors that could be placed on an integrated circuit would double every two years, or depending on one's source, every eighteen months. The transistor is a basic building block of engineering and computational capacity because it is the device that switches signals and electricity in

computers. The closer the transistors are to each other – hence microchips – the faster the computational speed. Moore's law captures both the specific point that microchip storage doubles every eighteen months to two years as well as the more general point that the pace of technological change is exponential and not linear, and it is getting faster all the time.

Because technology will always outpace the ability (or willingness) of Congress to legislate, statutory law should be technology neutral and not seek to dictate wise decisions through substantive prescript, but rather do so by requiring robust process and accountability. In other words, law should not tell decision-makers what to do, but rather describe a process of decision that is more likely to lead to wise choices. Remember, good process leads to better results.

What is more, the problem is not just that technology outpaces our ability to legislate and regulate, adversaries will learn to make use of new technology faster than the government typically makes policy or responds, a point made by former Deputy NSA Director Chris Inglis. Let us call this Inglis' Law. That means the law should not only contemplate the intended use of technology now, but the unintended and nefarious uses tomorrow by unknown actors.

Murphy's Law. "Murphy's law" is an aphorism that posits that if something can go wrong, it will. Apparently the "law" has been around for some time in different forms, and long before a Defense Department scientist named Murphy was associated with the concept. Whatever its origin it is a sound principle to keep in mind when building a legal framework to address emerging technologies that may, or may not, work as intended. History is full of examples of technological inventions that did not work as intended. Think of Icarus, the Mark 14 and 18 Torpedoes, Apollo 13, as well as Challenger and Columbia. The list goes on.

Murphy's Law argues for a legal framework that incorporates accountability, responsibility, and a process of ongoing review. The Foreign Intelligence Surveillance Act (FISA) is an example. It requires a court order for certain electronic surveillance on the front end; however, it also requires periodic review and renewal of Foreign Intelligence Surveillance Court orders, which orders validate the continued existence of a factual predicate, or probable cause, to continue the surveillance.

5. *A Technology Race Brings Predictable Risks*

A technological race brings predictable risks of the sorts associated with arms races. Arms races consume resources, and thus, potentially result in lost opportunity elsewhere. Arms races can also lead to risk taking, to keep up or to find an edge. Risk taking may come in the form of shortcuts, safety waivers, or reduced oversight to maintain security and preserve surprise. Arms races can also reduce cooperation and trust in other areas, like trade and diplomacy. Where an arms race in fact involves arms, it creates the further risk of their intended or accidental use. Of course, implicit in an arms race is the risk that if a nation does not keep pace and falls behind it may be placed in an untenable position of submission or surrender.

Law and policy should regulate these risks. In the case of law, this should be done with intentional reference to the three purposes of law – authority and boundaries, process, and values. Now.

VII. CONCLUSION

Emerging technologies like artificial intelligence and quantum computing are on the cusp of transforming national security practice. However, technology and the security threats posed by new technologies are exponentially outpacing any corresponding effort to articulate and implement a legal and ethical regime to regulate their wise and safe national security use. A technology arms race is on. So is the law and policy race. Will we understand and regulate the national security implications of these technologies before it is too late to do so effectively?

One of many things that makes the field of emerging technologies interesting and challenging from a governmental standpoint, is the necessity of responding in a horizontal as well as vertical fashion, across government and between federal, state, and local authorities. Moreover, although the government often speaks of "whole-of-government" approaches to national security problems, because of the importance of industry and academia, emerging technologies requires a "whole-of-country" approach. That requires good governance and process - in a word, law. It is time for lawyers and policymakers to take the lead and do something, conscious of the three purposes of law. The ABA-OSU Symposium, we hope, served as a positive step forward in doing so.